(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0112918
(43) 공개일자 2019년10월08일

(51) 국제특허분류(Int. Cl.)
*H04L 12/851* (2013.01) *H04L 12/823* (2013.01)
*H04L 12/893* (2013.01) *H04L 29/06* (2006.01)
(52) CPC특허분류
*H04L 47/2441* (2013.01)
*H04L 47/2433* (2013.01)
(21) 출원번호 10-2018-0034878
(22) 출원일자 2018년03월27일
심사청구일자 2018년03월27일

전체 청구항 수 : 총 20 항

(71) 출원인
**계명대학교 산학협력단**
대구광역시 달서구 달구벌대로 1095, 계명대학교 산학협력관 201호(신당동)
(72) 발명자
**박우길**
대구광역시 달서구 월서로 51 101동 1806호 (진천동, 월배역 포스코 더 샵 아파트)
(74) 대리인
**김건우**

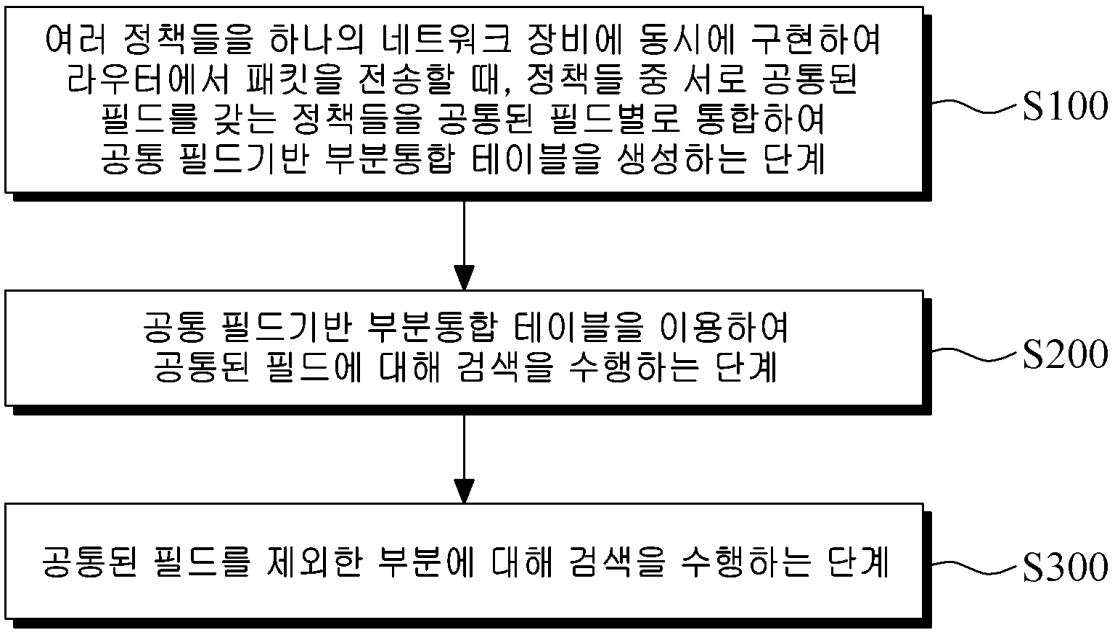
(54) 발명의 명칭 **고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법 및 시스템**

## (57) 요 약

본 발명은 패킷 분류 방법에 관한 것으로서, 보다 구체적으로는 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법에 있어서, 여러 정책들을 하나의 네트워크 장비에 동시에 구현하여 라우터에서 패킷을 전송하는 경우 여러 정책들 중 서로 공통된 필드를 갖는 정책들을 해당 필드별로 통합하는 단계; 상기 단계 (1)에서 통합된 공

(뒷면에 계속)

*대 표 도* - 도3



통되는 필드에 대해 검색을 하는 단계; 상기 단계 (2)에서 검색하지 않은 나머지 필드들에 대해 검색을 하는 단계; 및 상기 단계 (2) 및 (3)에 따른 검색 결과를 사용하여 정책의 우선순위대로 패킷을 처리하는 단계를 포함하는 것을 그 구성상의 특징으로 한다.

또한, 본 발명은 패킷 분류 시스템에 관한 것으로서, 보다 구체적으로는 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 시스템에 있어서, 여러 정책들 중 서로 공통되는 필드를 갖는 정책들을 해당 필드별로 통합하는 통합 모듈, 상기 통합 모듈에 의해 생성된 공통 필드기반 부분통합 테이블에 대해 검색하는 제1검색 모듈, 상기 제1검색 모듈에 의해 검색 되지 않은 나머지 필드들에 대해 검색하는 제2검색 모듈 및 상기 제1검색 모듈 및 제2검색 모듈에 따른 검색 결과를 사용하여 정책의 우선순위대로 패킷을 처리하는 패킷 처리 모듈을 포함하는 것을 그 구성상의 특징으로 한다.

본 발명에서 제안하고 있는 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법 및 시스템에 따르면, 정책들 중 서로 공통된 필드를 갖는 정책들을 공통된 필드별로 통합하여 공통 필드기반 부분통합 테이블을 생성함으로써, 각각의 검색 필드에 대해서 전체 정책들을 모두 검색하는데 단 한 번의 검색만이 필요하도록 하여, 테이블 크기나 테이블 생성 시간의 증가는 억제하면서 검색 성능을 크게 높일 수 있다.

또한, 본 발명에 따르면, 청크 테이블들이 기본적인 매칭 정책 정보와 함께 주어진 값에 대해 매칭 되는 정책이 존재하는지에 대한 정보를 동시에 가지고 있어, 매칭 되는 정책이 없는 경우 또는 패킷 전송 정책만 매칭 될 수 있는 경우 나머지 필드에 대한 테이블 검색을 생략함으로써, 불필요한 검색을 하지 않게 하여 검색 시간을 줄일 수 있다.

(52) CPC특허분류
*H04L 47/32* (2013.01)
*H04L 47/40* (2013.01)
*H04L 63/20* (2013.01)

# 명 세 서

## 청구범위

### 청구항 1

패킷을 분류하는 패킷 분류 방법에 있어서,

여러 정책들을 하나의 네트워크 장비에 동시에 구현하여 라우터에서 패킷을 전송하는 경우,

(1) 여러 정책들 중 서로 공통되는 필드를 갖는 정책들을 해당 필드별로 통합하는 단계;

(2) 상기 단계 (1)에서 통합된 공통되는 필드에 대해 검색을 하는 단계;

(3) 상기 단계 (2)에서 검색하지 않은 나머지 필드들에 대해 검색을 하는 단계; 및

(4) 상기 단계 (2) 및 (3)에 따른 검색 결과를 사용하여 정책의 우선순위대로 패킷을 처리하는 단계를 포함하는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법.

### 청구항 2

제1항에 있어서, 상기 단계 (1)은,

여러 정책들 중 각각의 검색 필드에 대해서 전체 정책들을 모두 검색하는데 단 한 번의 검색만이 필요하도록 공통 필드기반 부분통합 테이블을 생성하는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법.

### 청구항 3

제2항에 있어서, 상기 공통 필드기반 부분통합 테이블은,

청크와 청크비트맵 테이블을 포함하는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법.

### 청구항 4

제3항에 있어서, 상기 청크와 청크비트맵 테이블은,

기본적인 매칭 정책 정보와 함께 주어진 값에 대해 매칭 되는 정책이 존재하는지에 대한 정보를 동시에 가지고 있어 비매칭 정책 검색 회피기법을 사용할 수 있는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법.

### 청구항 5

제4항에 있어서, 상기 비매칭 정책 검색 회피기법은,

매칭 되는 정책이 없는 경우 또는 패킷 전송 정책만 매칭 될 수 있는 경우 나머지 필드에 대한 검색을 생략하게 하는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법.

### 청구항 6

제1항에 있어서, 상기 통합 패킷 분류 방법은,

상기 단계 (2)에서 통합된 공통되는 필드에 대한 검색 결과를 마지막에 사용하여 우선순위 문제를 해결하는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법.

**청구항 7**

제1항에 있어서, 상기 통합 패킷 분류 방법은,

각 정책 검색 테이블이 RFC로 구성될 수 있도록 하는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법.

**청구항 8**

제1항에 있어서, 상기 통합 패킷 분류 방법은,

소프트웨어 기반 방식으로 패킷 분류를 수행하는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법.

**청구항 9**

제1항에 있어서, 상기 통합 패킷 분류 방법은,

2개 이상의 정책을 하나의 네트워크 장비에서 동시에 구현하는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법.

**청구항 10**

제9항에 있어서, 상기 정책은,

IP SPOOFING 정책, ACL 정책, ROUTING 정책을 포함하는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법.

**청구항 11**

제1항에 있어서, 상기 공통된 필드는,

SOURCE IP 필드, DESTINATION IP 필드를 포함하는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법.

**청구항 12**

패킷을 분류하는 패킷 분류 시스템에 있어서,

여러 정책들을 하나의 네트워크 장비에 동시에 구현하여 라우터에서 패킷을 전송하는 경우,

(1) 여러 정책들 중 서로 공통되는 필드를 갖는 정책들을 해당 필드별로 통합하는 통합 모듈;

(2) 상기 단계 (1)에서 통합된 공통되는 필드에 대해 검색하는 제1검색 모듈 단계;

(3) 상기 단계 (2)에서 검색하지 않은 나머지 필드들에 대해 검색하는 제2검색 모듈; 및

(4) 상기 단계 (2) 및 (3)에 따른 검색 결과를 사용하여 정책의 우선순위대로 패킷을 처리하는 패킷 처리 모듈을 포함하는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 시스템.

**청구항 13**

제12항에 있어서, 상기 통합 모듈은,

여러 정책들 중 각각의 검색 필드에 대해서 전체 정책들을 모두 검색하는데 단 한 번의 검색만이 필요하도록 공통 필드기반 부분통합 테이블을 생성하는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 시스템.

**청구항 14**

제13항에 있어서, 상기 공통 필드기반 부분통합 테이블은,

청크와 청크비트맵 테이블을 포함하는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 시스템.

**청구항 15**

제14항에 있어서, 상기 청크와 청크비트맵 테이블은,

기본적인 매칭 정책 정보와 함께 주어진 값에 대해 매칭 되는 정책이 존재하는지에 대한 정보를 동시에 가지고 있어 비매칭 정책 검색 회피기법을 사용할 수 있는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 시스템.

**청구항 16**

제15항에 있어서, 상기 비매칭 정책 검색 회피기법은,

매칭 되는 정책이 없는 경우 또는 패킷 전송 정책만 매칭 될 수 있는 경우 나머지 필드에 대한 검색을 생략하게 하는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 시스템.

**청구항 17**

제12항에 있어서, 상기 통합 패킷 분류 시스템은,

상기 통합 모듈에서 통합된 공통되는 필드에 대한 검색 결과를 마지막에 사용하여 우선순위 문제를 해결하는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 시스템.

**청구항 18**

제12항에 있어서, 상기 통합 패킷 분류 시스템은,

각 정책 검색 테이블이 RFC로 구성될 수 있도록 하는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 시스템.

**청구항 19**

제12항에 있어서, 상기 통합 패킷 분류 시스템은,

소프트웨어 기반 방식으로 패킷 분류를 수행하는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 시스템.

**청구항 20**

제12항에 있어서, 상기 통합 패킷 분류 시스템은,

2개 이상의 정책을 하나의 네트워크 장비에서 동시에 구현하는 것을 특징으로 하는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 시스템.

## *발명의 설명*

### *기 술 분 야*

[0001] 본 발명은 패킷 분류 방법 및 시스템에 관한 것으로서, 보다 구체적으로는 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법 및 시스템에 관한 것이다.

### *배 경 기 술*

[0002] 라우터는 패킷 기반형 네트워크와 같은 주어진 통신 네트워크에 포함되는 정보 기술 장치이며, 주어진 네트워크와 적어도 하나의 접합을 제공하고, 주어진 네트워크를 통해 데이터 패킷을 유도하며, 주어진 네트워크로부터 다른 네트워크로 데이터 패킷을 전송하기 위한 것이다. 도 1은 라우터가 데이터 패킷을 주어진 네트워크로부터 다른 네트워크로 전송하는 모습을 나타낸 그림이다.

[0003] 현대의 네트워크는 IoT(Internet of Things)로 인해 크기가 대형화되고 있다. 이에 따라 정책 집합들이 복잡해지고, 그 크기와 개수 또한 빠르게 증가하고 있다. 이러한 대용량 보안 정책들로 인해, 높은 분류 속도와 작은 테이블 크기를 동시에 가질 수 있는 새로운 패킷 분류 알고리즘에 대한 요구가 높아지고 있다. 그러나 일반적으로 패킷 분류 속도와 테이블 크기는 Trade-off 관계를 가진다. 따라서 기술적으로 패킷 분류 알고리즘의 속도와 테이블 크기를 동시에 개선하는 것은 매우 어려운 실정이다.

[0004] 오늘날 인터넷 트래픽양이 폭증함에 따라 네트워크를 구성하는 장비들의 성능도 크게 발전하고 있다. 특히, 네트워크의 기본 장비인 라우터에 요구되는 패킷 전송 성능 역시 빠르게 증가하고 있다. 라우터의 성능을 높이기 위해서는, 목적지 주소를 키로 검색할 수 있도록 T-CAM(Temary Content Addressable Memory)를 이용하는 것이 가장 일반적인 구현 방법이다.

[0005] 한편, 다양한 사이버 보안 공격들이 발생하면서 이들로부터 네트워크를 방어하기 위해 라우터에 일부 보안 기능들이 추가되고 있다. 예를 들면, ACL(Access Control List)과 NAT(Network Address Translation), 안티 IP 스푸핑(Anti IP Spoofing) 등이 대표적인 기능이다. 도 2는 라우터에서 사용되는 일반적인 보안 정책들의 알고리즘을 나타낸 도면이다. 도 2를 통해, (a) IP SPOOFING 정책, (b) ROUTING 정책, (c) ACL 정책의 알고리즘을 확인할 수 있다. 이와 같은 기능들은 각각 IP 검색과 달리 발송지 IP 주소, 발송지 포트 번호, 목적지 포트 번호, 프로토콜 값 등 총 5개의 키를 사용하여 매칭 되는 정책들 중 가장 우선순위가 높은 정책에 따라 패킷을 처리하는 패킷 분류 방식을 주로 사용한다.

[0006] 이와 같이 다양한 보안 기능들을 제공하면서 라우터의 전송 성능을 유지한다는 것은 기술적으로 상당히 어렵다. 지금까지 이를 해결하기 위한 방법은 각 정책 집합별 검색 성능을 향상함으로써 전체 시스템의 성능을 높이는 것이었다. 하지만, 이 방식은 라우터에 요구되는 보안 기능이 증가하고 있는 현 상황에서는 근본적인 해결책이라고 할 수 없다. 보안 기능의 수가 증가함에 따라 수신된 패킷을 처리하는데 수행되어야하는 패킷 분류의 수가 증가하게 되고 이에 따라 결국 전체 라우터의 성능은 감소하기 때문이다.

[0007] 최근에는 RFC(Recursive Flow Classification)와 같은 cross-producting 기반 알고리즘의 대형 검색 테이블을 사용함으로써 라우팅뿐만 아니라 5 튜플을 사용하는 보안 기능 내 정책 검색 기능까지 지원이 가능하다. RFC를

사용하면 무엇보다도 정책의 수에 상관없이 고정된 검색 성능을 갖는다는 장점이 있다. 하지만 정책이 커질 경우 테이블의 크기가 증가하게 되어 테이블 생성 시간이 길어져 실제 네트워크상에서 사용할 수 없다는 단점이 있다.

[0008] 한편, 이와 관련된 선행기술로는, 등록특허 제10-1331018호(발명의 명칭: 패킷 분류 방법 및 그 장치)와 등록특허 제10-0451788호(발명의 명칭: VPN라우터의 LNS 성능향상을 위한 L2TP 패킷고속 수신방법) 등이 제시된 바 있다.

## 발명의 내용

### 해결하려는 과제

[0009] 본 발명은 기존에 제안된 방법들의 상기와 같은 문제점들을 해결하기 위해 제안된 것으로서, 여러 정책들을 하나의 네트워크 장비에 동시에 구현하여 라우터에서 패킷을 전송하는 경우, 정책들 중 서로 공통된 필드를 갖는 정책들을 공통된 필드별로 통합하여 공통 필드기반 부분통합 테이블을 생성함으로써, 각각의 검색 필드에 대해서 전체 정책들을 모두 검색하는데 단 한 번의 검색만이 필요하도록 하여, 테이블 크기나 테이블 생성 시간의 증가는 억제하면서 검색 성능을 크게 높일 수 있는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법 및 시스템을 제공하는 것을 목적으로 한다.

[0010] 또한, 본 발명은, 청크 테이블들이 기본적인 매칭 정책 정보와 함께 주어진 값에 대해 매칭 되는 정책이 존재하는지에 대한 정보를 동시에 가지고 있어, 매칭 되는 정책이 없는 경우 또는 패킷 전송 정책만 매칭 될 수 있는 경우 나머지 필드에 대한 테이블 검색을 생략함으로써, 불필요한 검색을 하지 않게 하여 검색 시간을 줄일 수 있는, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법 및 시스템을 제공하는 것을 다른 목적으로 한다.

### 과제의 해결 수단

[0011] 상기한 목적을 달성하기 위한 본 발명의 특징에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법은,

[0012] 패킷을 분류하는 패킷 분류 방법에 있어서,

[0013] 여러 정책들을 하나의 네트워크 장비에 동시에 구현하여 라우터에서 패킷을 전송하는 경우,

[0014] (1) 여러 정책들 중 서로 공통되는 필드를 갖는 정책들을 해당 필드별로 통합하는 단계;

[0015] (2) 상기 단계 (1)에서 통합된 공통되는 필드에 대해 검색을 하는 단계;

[0016] (3) 상기 단계 (2)에서 검색하지 않은 나머지 필드들에 대해 검색을 하는 단계; 및

[0017] (4) 상기 단계 (2) 및 (3)에 따른 검색 결과를 사용하여 정책의 우선순위대로 패킷을 처리하는 단계를 포함하는 것을 그 구성상의 특징으로 한다.

[0018] 바람직하게는, 상기 단계 (1)은,

[0019] 여러 정책들 중 각각의 검색 필드에 대해서 전체 정책들을 모두 검색하는데 단 한 번의 검색만이 필요하도록 공통 필드기반 부분통합 테이블을 생성할 수 있다.

[0020] 더욱 바람직하게는, 상기 공통 필드기반 부분통합 테이블은,

[0021] 청크와 청크비트맵 테이블을 포함할 수 있다.

[0022] 더욱더 바람직하게는, 상기 청크와 청크비트맵 테이블은,

[0023] 기본적인 매칭 정책 정보와 함께 주어진 값에 대해 매칭 되는 정책이 존재하는지에 대한 정보를 동시에 가지고 있어 비매칭 정책 검색 회피기법을 사용할 수 있다.

[0024] 더욱더 바람직하게는, 상기 비매칭 정책 검색 회피기법은,

[0025] 매칭 되는 정책이 없는 경우 또는 패킷 전송 정책만 매칭 될 수 있는 경우 나머지 필드에 대한 검색을 생략하게 할 수 있다.

[0026] 바람직하게는, 상기 통합 패킷 분류 방법은,

[0027] 상기 단계 (2)에서 통합된 공통되는 필드에 대한 검색 결과를 마지막에 사용하여 우선순위 문제를 해결할 수 있다.

[0028] 바람직하게는, 상기 통합 패킷 분류 방법은,

[0029] 각 정책 검색 테이블이 RFC로 구성될 수 있다.

[0030] 바람직하게는, 상기 통합 패킷 분류 방법은,

[0031] 소프트웨어 기반 방식으로 패킷 분류를 수행할 수 있다.

[0032] 바람직하게는, 상기 통합 패킷 분류 방법은,

[0033] 2개 이상의 정책을 하나의 네트워크 장비에서 동시에 구현할 수 있다.

[0034] 더 바람직하게는, 상기 정책은,

[0035] IP SPOOFING 정책, ACL 정책, ROUTING 정책을 포함할 수 있다.

[0036] 바람직하게는, 상기 공통된 필드는,

[0037] SOURCE IP 필드, DESTINATION IP 필드를 포함할 수 있다.

[0038] 또한, 상기한 목적을 달성하기 위한 본 발명의 특징에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 시스템은,

[0039] 패킷을 분류하는 패킷 분류 시스템에 있어서,

[0040] 여러 정책들을 하나의 네트워크 장비에 동시에 구현하여 라우터에서 패킷을 전송하는 경우,

[0041] (1) 여러 정책들 중 서로 공통되는 필드를 갖는 정책들을 해당 필드별로 통합하는 통합 모듈;

[0042] (2) 상기 단계 (1)에서 통합된 공통되는 필드에 대해 검색하는 제1검색 모듈 단계;

[0043] (3) 상기 단계 (2)에서 검색하지 않은 나머지 필드들에 대해 검색하는 제2검색 모듈; 및

[0044] (4) 상기 단계 (2) 및 (3)에 따른 검색 결과를 사용하여 정책의 우선순위대로 패킷을 처리하는 패킷 처리 모듈을 포함하는 것을 그 구성상의 특징으로 한다.

[0045] 바람직하게는, 상기 통합 모듈은,

[0046] 여러 정책들 중 각각의 검색 필드에 대해서 전체 정책들을 모두 검색하는데 단 한 번의 검색만이 필요하도록 공통 필드기반 부분통합 테이블을 생성할 수 있다.

[0047] 더 바람직하게는, 상기 공통 필드기반 부분통합 테이블은,

[0048] 청크와 청크비트맵 테이블을 포함할 수 있다.

[0049] 더욱더 바람직하게는, 상기 청크와 청크비트맵 테이블은,

[0050] 기본적인 매칭 정책 정보와 함께 주어진 값에 대해 매칭 되는 정책이 존재하는지에 대한 정보를 동시에 가지고 있어 비매칭 정책 검색 회피기법을 사용할 수 있다.

[0051] 더욱더 바람직하게는, 상기 비매칭 정책 검색 회피기법은,

[0052] 매칭 되는 정책이 없는 경우 또는 패킷 전송 정책만 매칭 될 수 있는 경우 나머지 필드에 대한 검색을 생략하게 할 수 있다.

[0053] 바람직하게는, 상기 통합 패킷 분류 시스템은,

[0054] 상기 통합 모듈에서 통합된 공통되는 필드에 대한 검색 결과를 마지막에 사용하여 우선순위 문제를 해결할 수 있다.

[0055] 바람직하게는, 상기 통합 패킷 분류 시스템은,

[0056] 각 정책 검색 테이블이 RFC로 구성될 수 있다.

[0057] 바람직하게는, 상기 통합 패킷 분류 시스템은,

[0058] 소프트웨어 기반 방식으로 패킷 분류를 수행할 수 있다.

[0059] 바람직하게는, 상기 통합 패킷 분류 시스템은,

[0060] 2개 이상의 정책을 하나의 네트워크 장비에서 동시에 구현할 수 있다.

## *발명의 효과*

[0061] 본 발명에서 제안하고 있는 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법 및 시스템에 따르면, 여러 정책들을 하나의 네트워크 장비에 동시에 구현하여 라우터에서 패킷을 전송하는 경우, 정책들 중 서로 공통된 필드를 갖는 정책들을 공통된 필드별로 통합하여 공통 필드기반 부분통합 테이블을 생성함으로써, 각각의 검색 필드에 대해서 전체 정책들을 모두 검색하는데 단 한 번의 검색만이 필요하도록 하여, 테이블 크기나 테이블 생성 시간의 증가는 억제하면서 검색 성능을 크게 높일 수 있다.

[0062] 또한, 본 발명에 따르면, 청크 테이블들이 기본적인 매칭 정책 정보와 함께 주어진 값에 대해 매칭 되는 정책이 존재하는지에 대한 정보를 동시에 가지고 있어, 매칭 되는 정책이 없는 경우 또는 패킷 전송 정책만 매칭 될 수 있는 경우 나머지 필드에 대한 테이블 검색을 생략함으로써, 불필요한 검색을 하지 않게 하여 검색 시간을 줄일 수 있다.

## *도면의 간단한 설명*

[0063] 도 1은 라우터가 데이터 패킷을 주어진 네트워크로부터 다른 네트워크로 전송하는 모습을 나타낸 그림.

도 2는 라우터에서 사용되는 일반적인 보안 정책들의 알고리즘을 나타낸 도면.

도 3은 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법의 구성을 도시한 도면.

도 4는 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법에서 여러 정책 집합을 하나의 네트워크 장비에서 동시에 구현하는 경우 겹치는 필드가 존재한다는 것을 나타내기 위한 도면.

도 5는 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법을 RFC에 적용한 경우의 테이블 구성을 나타낸 도면.

도 6은 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법의 알고리즘을 도시한 도면.

도 7은 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법을 RFC 방식에 구현하고 라우팅 정책 수에 따른 테이블 크기의 값을 도시한 도면.

도 8은 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법을 RFC 방식에 구현하고 라우팅 정책 수에 따른 메모리 액세스 수의 값을 도시한 도면.

도 9는 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법을 RFC 방식에 구현하고 라우팅 정책 수에 따른 테이블 생성 시간 값을 도시한 도면.

도 10은 본 발명의 다른 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 시스템(100)의 세부 구성을 도시한 도면.

## *발명을 실시하기 위한 구체적인 내용*

[0064] 이하에서는 첨부된 도면을 참조하여 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있도록 바람직한 실시예를 상세히 설명한다. 다만, 본 발명의 바람직한 실시예를 상세하게 설명함에 있어, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략한다. 또한, 유사한 기능 및 작용을 하는 부분에 대해서는 도면 전체에 걸쳐 동일 또는 유사한 부호를 사용한다.

[0065] 덧붙여, 명세서 전체에서, 어떤 부분이 다른 부분과 '연결' 되어 있다고 할 때, 이는 '직접적으로 연결' 되어 있는 경우뿐만 아니라, 그 중간에 다른 소자를 사이에 두고 '간접적으로 연결' 되어 있는 경우도 포함한다. 또한, 어떤 구성요소를 '포함' 한다는 것은, 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있다는 것을 의미한다.

[0066] 도 3은 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법의 구성을 도시한 도면이다. .도 3에 도시된 바와 같이, 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법은, 패킷을 분류하는 패킷 분류 방법에 있어서, 여러 정책들을 하나의 네트워크 장비에 동시에 구현하여 라우터에서 패킷을 전송하는 경우, (1) 여러 정책들 중 서로 공통되는 필드를 갖는 정책들을 해당 필드별로 통합하는 단계(S100); (2) 상기 단계 (1)에서 통합된 공통되는 필드에 대해 검색을 하는 단계(S200); (3) 상기 단계 (2)에서 검색하지 않은 나머지 필드들에 대해 검색하는 단계(S300); 및 (4) 상기 단계 (2) 및 (3)에 따른 검색 결과를 사용하여 정책의 우선순위대로 패킷을 처리하는 단계(S400)를 포함할 수 있다. 이하에서는 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법의 각각의 구성에 대해 상세히 설명하기로 한다.

[0067] 단계 S100에서는, 여러 정책들을 하나의 네트워크 장비에 동시에 구현하여 라우터에서 패킷을 전송하는 경우, 여러 정책들 중 서로 공통되는 필드를 갖는 정책들을 해당 필드별로 통합할 수 있다. 도 4는 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법에서 여러 정책 집합을 하나의 네트워크

장비에서 동시에 구현하는 경우 겹치는 필드가 존재한다는 것을 나타내기 위한 도면이다. 도 4에 도시된 바와 같이, A 정책과 그에 속하는 a 필드, B 정책과 그에 속하는 a, b, c, d 필드, 그리고 C 정책과 그에 속하는 c, f 필드가 있다고 할 때, A 정책과 B 정책에 대해서는 a 필드가 겹치고, B 정책과 C 정책에 대해서는 c 필드가 겹칠 수 있다. 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법에서는 각각의 검색 필드에 대해서 전체 정책들을 모두 검색하는데 단 한 번의 검색만이 필요하도록 테이블을 구성하게 되도록 서로 공통된 필드를 갖는 정책들을 해당 필드별로 통합하여 공통 필드기반 부분통합 테이블을 생성할 수 있다. 이렇게 함으로써, 원래의 경우 a 필드는 A 정책과 B 정책에 공통적으로 존재하므로 a 필드에 대해 두 번의 검색을 하였지만, 두 정책 테이블에서 a 필드에 대해 부분적으로 통합하여 a 필드에 대해 한 번의 검색만이 필요하게 된다.

[0068] 단계 S200에서는, 단계 S100에서 생성된 공통 필드기반 부분통합 테이블을 이용하여 공통된 필드에 대해 검색을 수행할 수 있다. 즉, 여러 정책 중 겹치는 필드인 a 필드와 c 필드에 대해 검색을 수행하여 결과를 얻을 수 있다.

[0069] 단계 S300에서는, 단계 S200에서 검색하지 않은 나머지 필드들에 대해 검색할 수 있다. 이로써 겹치지 않은 b, d, f 필드에 대한 검색 결과를 얻을 수 있다. 본 발명에서 제안하고 있는 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법은, 매칭 되는 정책들 중 우선순위가 높은 정책에 따라 패킷을 처리하는 분류 방식을 사용할 수 있다. 공통 필드기반 부분통합 테이블을 생성하여 검색을 수행하면 우선순위 문제가 발생할 수 있다. 예를 들어, B 정책의 우선순위가 C 정책보다 높다고 가정하면 이와 같은 공통 필드기반 부분통합 테이블에서는 우선순위가 낮은 정책의 결과를 먼저 얻을 수 있다. 하지만 모든 필드에 대한 검색을 마친 후에는 모든 정책에 대한 검색 결과를 얻게 되므로 미리 얻은 결과를 마지막에 사용하도록 함으로써 우선순위 문제를 해결 할 수 있다.

[0070] 도 5는 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법을 RFC에 적용한 경우의 테이블 구성을 나타낸 도면이다. 도 5에 도시된 바와 같이, 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법을 RFC에 적용하여 청크와 청크비트맵(CBM) 테이블을 생성할 수 있다. 앞서 설명한 것처럼, A 정책과 B 정책은 a 필드를, B 정책과 C 정책은 c 필드를 공통필드로 가지고 있다. 따라서 통합 RFC 테이블에서 a 필드 관련 청크 테이블의 경우 A 정책과 B 정책을 하나의 정책으로 합친 후 생성될 수 있다. 또한, c 필드 관련 청크 테이블은 B 정책과 C 정책을 하나의 정책으로 합친 후 생성될 수 있다.

[0071] 이때, 청크 테이블들은 기본적인 매칭 정책 정보와 함께 주어진 값에 대해 매칭 되는 정책이 존재하는지에 대한 정보를 동시에 가지고 있어 비매칭 검색 회피기법을 사용할 수 있다. 상기 비매칭 정책 검색 회피기법은 매칭 되는 정책이 없는 경우 또는 패킷 전송 정책만 매칭 될 수 있는 경우 나머지 필드에 대한 테이블 검색을 생략함으로써, 불필요한 검색을 하지 않게 할 수 있다. 예를 들어, 기존 청크 테이블의 각각의 엔트리는 Equivalence ID(eqID)값을 갖지만 통합된 청크 테이블의 테이블 엔트리는 정책 A 중 매칭된 룰 번호가 추가된 eqID 값을 갖는다. 또한, 정책 B에 대한 eqID는 비트맵의 모든 비트가 0으로 설정된 비트맵을 가리킬 경우 미리 지정된 값으로 설정될 수 있다. 따라서 두 청크 테이블의 eqID 중 하나라도 미리 지정된 값이 되면 나머지 필드에 대한 검색이 생략될 수 있다.

[0072] 도 6은 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법의 알고리즘을 도시한 도면이다. 도 6에 도시된 바와 같이, 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법은 공통 필드기반 부분통합 테이블에 대해 먼저 검색을 한 후, 검색하지 않은 나머지 필드들에 대해 검색을 할 수 있다.

[0073] 이하에서는 도 7 내지 도 9를 참조하여, 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법의 성능을 비교한다. 성능 평가를 위해 IP SPOOFING 정책과 그에 속하는 Sourece IP(SIP) 필드, ROUTING 정책과 그에 속하는 Destination IP(DIP) 필드, 그리고 ACL 정책과 그에 속하는 SIP, DIP, SPORT,

DPORT, PROTO를 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법과 기존 RFC 방식으로 구현하고, ROUTING 정책 수에 따른 테이블 크기, 메모리 액세스 수, 그리고 테이블 생성 시간을 측정하였다. 성능 측정을 위한 패킷은 무작위로 생성하였으며, 10회 반복 후 평균 성능을 측정하였다. 비교대상으로는 IP SPOOFING 정책, ACL 정책, ROUTING 정책에 대해 독립적으로 테이블을 생성한 경우와 모든 정책을 하나의 큰 정책으로 통합한 후 하나의 테이블을 생성하는 경우를 선택하였다.

[0074] 도 7은 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법을 RFC 방식에 구현하고 라우팅 정책 수에 따른 테이블 크기의 값을 도시한 도면이다. 도 7에 도시된 바와 같이, 통합정책 테이블을 사용하는 경우에는 테이블 크기가 지나치게 커짐을 알 수 있다. 따라서 실제 라우터에 적용하기에는 불가능하다. 반면, 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법을 사용한 경우에는, 독립 테이블에 비해 룰 수가 40,000인 경우 70% 정도 큰 테이블크기를 갖는다. 다만, 룰 수가 작을수록 테이블 크기 차이가 감소하기 때문에 룰 수가 20,000개인 경우 50% 정도, 10,000개인 경우 40% 정도 큰 테이블을 갖는다. 룰 수가 40,000개인 경우에도 전체 테이블 크기는 60KB 정도밖에 안되므로 실제 사용하는데 큰 무리가 없다.

[0075] 도 8은 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법을 RFC 방식에 구현하고 라우팅 정책 수에 따른 메모리 액세스 수의 값을 도시한 도면이다. 도 8에 도시된 바와 같이, 메모리 액세스 수는 모든 정책을 하나로 합친 경우에는 13, 3개의 정책에 대해 독립적으로 테이블을 생성한 경우에는 19이다. 반면, 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법의 경우에는, 13 이하의 메모리 액세스를 사용하는 것을 알 수 있다. ACL 정책의 룰 수가 증가할수록 전체적인 메모리 액세스 수는 증가하여 13에 가깝게 되지만, ACL 정책의 수가 적은 경우 통합 정책 방식에 비해서 2배 높은 성능을 가진다. 즉, 하나의 ACL 정책을 검색하는 것보다도 빠르게 세 정책을 검색할 수 있으므로, 다중 정책집합을 사용하는데 본 발명에서 제안하고 있는 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법이 매우 탁월함을 알 수 있다.

[0076] 도 9는 본 발명의 일 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법을 RFC 방식에 구현하고 라우팅 정책 수에 따른 테이블 생성 시간 값을 도시한 도면이다. 도 9에 도시된 바와 같이, 테이블 생성 시간은 통합정책 방식의 경우 시간이 지나치게 오래 걸리기 때문에 실제 측정이 아닌 추정시간을 대신 나타내었다. 독립된 정책을 사용하는 경우 테이블 크기가 가장 작게 된다. 하지만, 본 발명에서 제안하고 있는 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법의 경우 독립된 정책을 사용하는 경우와 비교한다 해도 그 차이가 미비하다고 볼 수 있다.

[0077] 도 10은 본 발명의 다른 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 시스템(100)의 세부 구성을 도시한 도면이다. 도 10에 도시된 바와 같이, 본 발명의 다른 실시예에 따른 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 시스템은, 통합 모듈(110), 제1검색 모듈(120), 제2검색 모듈(130), 및 패킷 처리 모듈(140)을 포함할 수 있다.

[0078] 통합 모듈(110)은, 패킷 분류시스템에 있어서, 여러 정책들을 하나의 네트워크 장비에 구현하여 라우터에서 패킷을 전송하는 경우 여러 정책들 중 서로 공통되는 필드를 갖는 정책들을 해당 필드별로 통합할 수 있다. 제1검색 모듈(120)은, 통합 모듈(110)에 의해 생성된 공통 필드기반 부분통합 테이블에 대해 검색할 수 있다. 제2검색 모듈(130)은, 제1검색 모듈(120)에 의해 검색이 되지 않은 나머지 필드들에 대해 검색을 할 수 있다. 패킷 처리 모듈(140)은, 제1검색 모듈(120) 및 제2검색 모듈(130)에 따른 검색 결과를 사용하여 정책의 우선순위대로 패킷을 처리할 수 있다.

[0079] 각각의 구성들과 관련된 상세한 내용들은, 앞서 본 발명의 일실시예에 따른 고성능 보안 라우터를 지원하기 위

한 통합 패킷 분류 방법과 관련하여 충분히 설명되었으므로, 상세한 설명은 생략하기로 한다.

[0080] 상술한 바와 같이, 본 발명에서 제안하고 있는 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 방법 및 시스템에 따르면, 여러 정책들을 하나의 네트워크 장비에 동시에 구현하여 라우터에서 패킷을 전송하는 경우, 정책들 중 서로 공통된 필드를 갖는 정책들을 공통된 필드별로 통합하여 공통 필드기반 부분통합 테이블을 생성함으로써, 각각의 검색 필드에 대해서 전체 정책들을 모두 검색하는데 단 한 번의 검색만이 필요하도록 하여, 테이블 크기나 테이블 생성 시간의 증가는 억제하면서 검색 성능을 크게 높일 수 있다. 또한, 본 발명에 따르면, 청크 테이블들이 기본적인 매칭 정책 정보와 함께 주어진 값에 대해 매칭 되는 정책이 존재하는지에 대한 정보를 동시에 가지고 있어, 매칭 되는 정책이 없는 경우 또는 패킷 전송 정책만 매칭 될 수 있는 경우 나머지 필드에 대한 테이블 검색을 생략함으로써, 불필요한 검색을 하지 않게 하여 검색 시간을 줄일 수 있다.

[0081] 이상 설명한 본 발명은 본 발명이 속한 기술분야에서 통상의 지식을 가진 자에 의하여 다양한 변형이나 응용이 가능하며, 본 발명에 따른 기술적 사상의 범위는 아래의 청구범위에 의하여 정해져야 할 것이다.

## *부호의 설명*

[0082] 100: 고성능 보안 라우터를 지원하기 위한 통합 패킷 분류 시스템

110: 통합 모듈

120: 제1검색 모듈

130: 제2검색 모듈

140: 패킷 처리 모듈

S100: 여러 정책들 중 서로 공통되는 필드를 갖는 정책들을 해당 필드별로 통합하는 단계

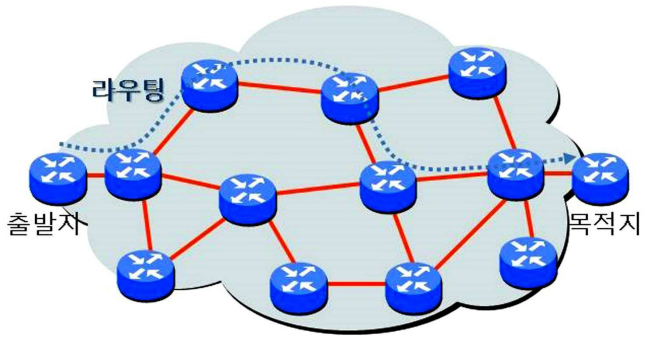
S200: 단계 S100에서 통합된 공통되는 필드에 대해 검색을 하는 단계

S300: 단계 S200에서 검색하지 않은 나머지 필드들에 대해 검색하는 단계

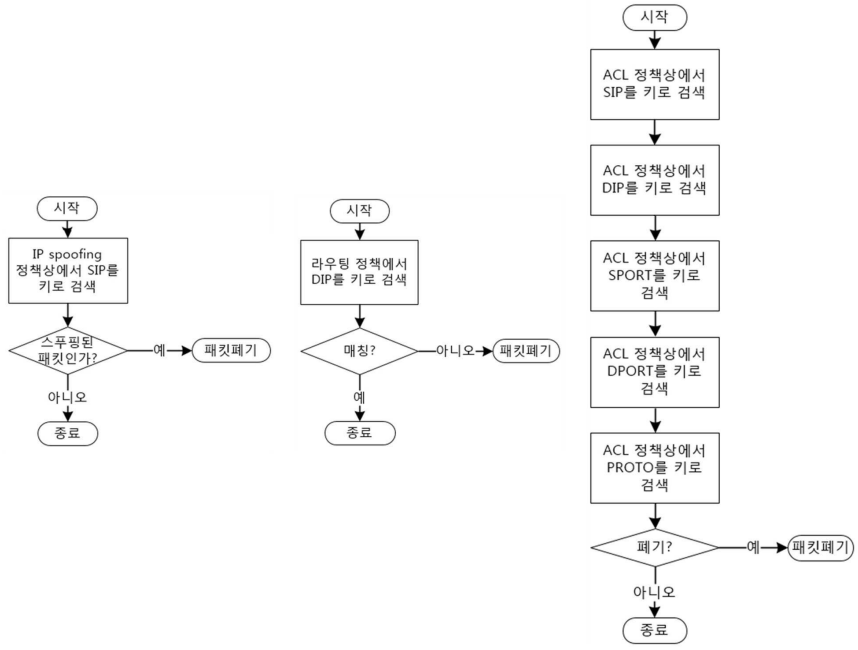
S400: 단계 S200 및 S300에 따른 검색 결과를 사용하여 정책의 우선순위대로 패킷을 처리 하는 단계

## *도면*

### *도면1*

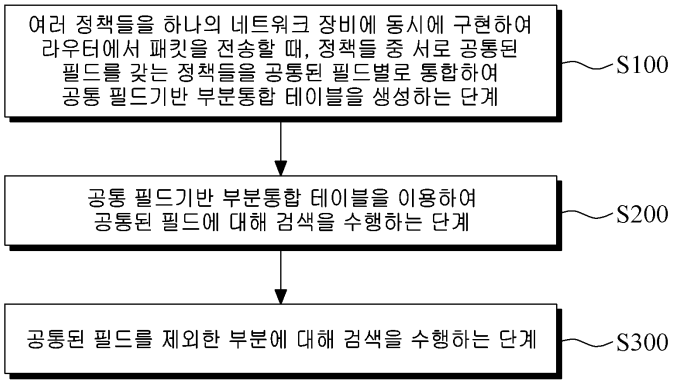


도면2

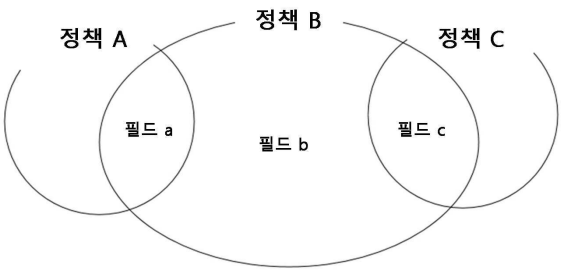



(a) IP SPOOFING 정책 (b) ROUTING 정책 (c) ACL 정책

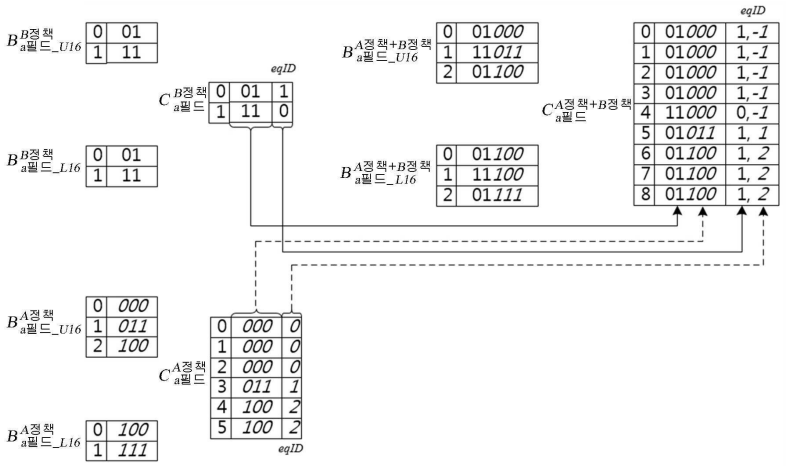
도면3



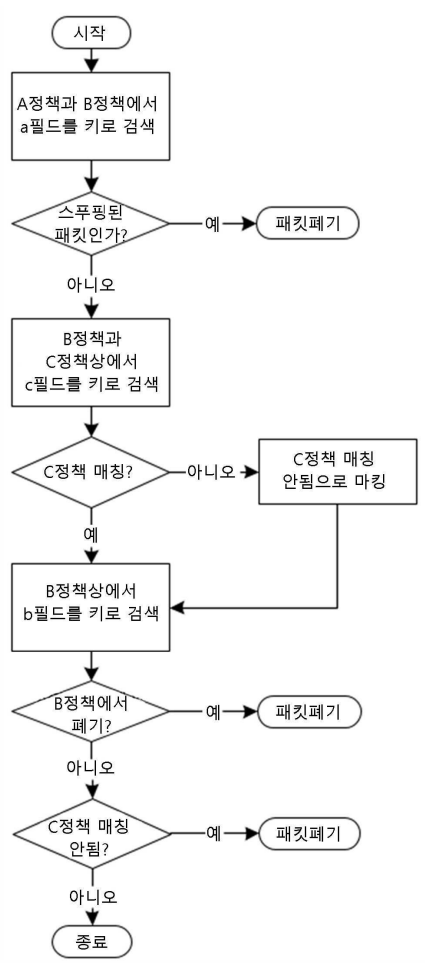

도면4



도면5


eqID
eqID
eqID

도면6


시작
A정책과 B정책에서 a필드를 키로 검색
스푸핑된 패킷인가?
예
패킷폐기
아니오
B정책과 C정책상에서 c필드를 키로 검색
C정책 매칭?
아니오
C정책 매칭 안됨으로 마킹
예
B정책상에서 b필드를 키로 검색
B정책에서 폐기?
예
패킷폐기
아니오
C정책 매칭 안됨?
예
패킷폐기
아니오
종료

도면7

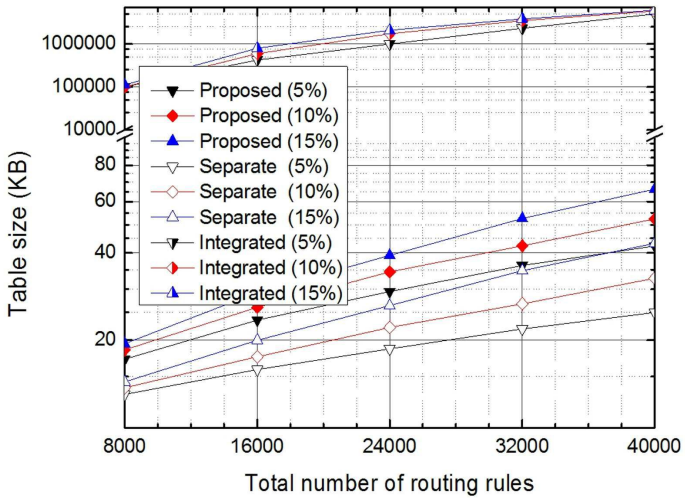
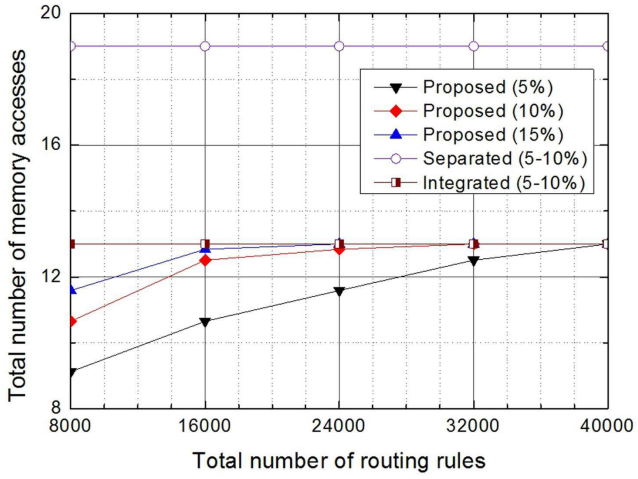


Table size (KB)
1000000
100000
10000
80
60
40
20
Proposed (5%)
Proposed (10%)
Proposed (15%)
Separate (5%)
Separate (10%)
Separate (15%)
Integrated (5%)
Integrated (10%)
Integrated (15%)
8000
16000
24000
32000
40000
Total number of routing rules

도면8


Total number of memory accesses
20
16
12
8
Proposed (5%)
Proposed (10%)
Proposed (15%)
Separated (5-10%)
Integrated (5-10%)
8000
16000
24000
32000
40000
Total number of routing rules

도면9

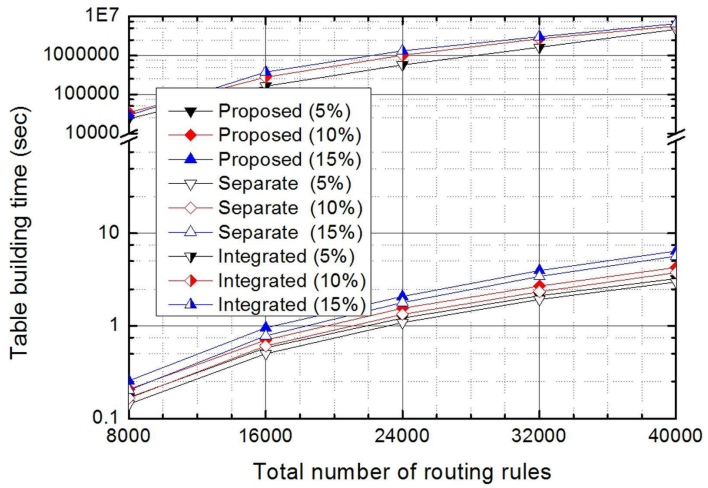


Table building time (sec)
1E7
1000000
100000
10000
10
1
0.1
Proposed (5%)
Proposed (10%)
Proposed (15%)
Separate (5%)
Separate (10%)
Separate (15%)
Integrated (5%)
Integrated (10%)
Integrated (15%)
8000
16000
24000
32000
40000
Total number of routing rules

도면10